UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/770,525	01/25/2001	Michael Hrabik	881075/3	5856

7590 01/30/2006

Joel E. Lutzker, Esq.
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, NY 10022

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/770,525	HRABIK ET AL.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *23,25,28-30,32,33,35,39-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *23,25,28-30,32,33,35 and 39-41* is/are rejected.

7)☒ Claim(s) *31 and 36-38* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20061101*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Office Action

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 23, 25, 28-30, 33, 39-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Emigh in view of Messmer.

3. As per claims 23, 30, 33, 39, Emigh teaches a security system(i.e. netranger sensor) for a computer network, the network having a plurality of devices connected thereto (see lines 1-4, 28-30), a security subsystem connected to at least some of the devices in the network(see lines 28-30), the security subsystem configured to monitor activities of the at least some devices on the network(see lines 28-32), and detect attacks on the at least some devices(see lines 33-36); a master system(i.e. IBM's Network Security Operations Center(NSOC) which monitors the integrity of the security subsystem and registers information pertaining to attacks detected by the security subsystem(see lines 1-6, 37-43); Emigh teaches that if a misuse is found it can be sent in real-time to the NSOC in Boulder, Colorado(see lines 33-36), connected between the security subsystem and the master system(see lines 33-36), the master system monitoring the integrity of the security subsystem and receiving the information pertaining to the attacks (see lines 1-6, 37-43). Emigh is silent on a secure link. Messmer teaches the link it output in encrypted form(i.e. vpn). It would have been obvious to one of ordinary skill in the art at the time of the invention to include a secure link by a virtual private network tunnel of Messmer with Emigh, the motivation

is that network activity is output in encrypted form and prevents hackers or intruders from viewing information(see Messmer).

4. As per claim 25, Emigh teaches the master system does not take direction from the security subsystem, because Emigh teaches the NSOC is a separate and independent network, that provides monitoring services to corporate networks(see pg. 1).

5. As per claim 28, Emigh teaches the master system is hierarchically independent from the security subsystem(see lines 1-6).

6. As per claim 29, Emigh teaches that the security subsystem is hierarchically subordinate to the master system(see lines 28-32).

7. As per claims 40, Emigh inherently teaches at lest one of the devices having a security related functions is a firewall, because Emigh teaches that the sensor can be located on places of the internet or intranet connections (see lines 28-32).

8. As per claim 41, Emigh teaches wherein at least one of the devices having security related functions is a network intrusion detection system(see lines 1-6).

9. Claims 32, 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Emigh in view of Messmer and further in view of Kurtzberg.

10. As per claim 32, 35, Emigh-Messmer combination teaches a master system(see lines 5-6), security subsystem(see lines 1-4), detecting attacks(see lines 33-36). Emigh-Messmer combination does not teach a pseudo-attack generator, which generates attacks on the network, and determining whether the integrity of the system has been compromised. Kurtzberg et al. discloses a pseudo-attack generator, which generates attacks on the network, and determining whether the integrity of the system has been compromised (see col. 1, lines 40-67). It would

have been obvious to one of ordinary skill in the art at the time of the invention to include a pseudo-attack generator which generates attacks on the network, and determining whether the integrity of the system has been compromised of Kurtzberg with Emigh-Messmer combination, the motivation if that the integrity of a computer system can be tested reliably to improve or complement the system's performance (see col. 1, lines 65-67 of Kurtzberg).

11. Claims 31, 36, 37-38 are objected to as being rejected on base claims. The reasons why the claims are allowable are because in the prior art of security, networking and non-patent literature, prior art fails to disclose or suggest, when the master system monitors whether the security subsystem responds to the master system, the master system taking action. The master system monitors the security subsystem in prior art and all data for network devices is transmitted to the master system, there is no suggestion or disclosure of this limitation.

Response to Amendment

12. The Applicant has requested an interview prior to formal action on this amendment. The Applicant was informed months ago that any additional interview was at the discretion of the Examiner. The Applicant has asserted that the grounds of the rejection were substantially changed from the rejections based on Messmer to rejections based on Emigh. However, the Examiner has conducted several interviews between the Attorney of Record, and the Inventor. The last interview was conducted on May 12, 2005. The rejection mailed on 6/2/05 contained no substantial changes to the claims(claims dated 2/28/05) of record, and scope of the claims of record were not changed the same art was applied. Further, the claims submitted 8/15/05 contain no substantial changes that would warrant another interview in regards to this application, and same art was applied to claims. The claims dated 12/19/05 also contain no

substantial changes that would warrant another interview. The Examiner has conducted several interviews in regards to this Application already.

713.01 [R-3] General Policy, How Conducted

37 CFR 1.133. Interviews.

13. An interview should be had only when the nature of the case is such that the interview could serve to develop and clarify specific issues and lead to a mutual understanding between the examiner and the applicant, and thereby advance the prosecution of the application. Therefore, the Applicant has not amended the claims substantially, the only amendments made were to overcome 112 rejection, and claim 25 in which the Applicant actually remove/deleted limitations from dependent claim 25. The same art was applied to the claims as per the previous rejections(see remarks above), and interviews were previously conducted on the rejections based on the art applied. The Examiner continues to rely on the prior art used to reject claims, because the Applicant's arguments have been unpersuasive. Further, the Applicant has made no significant changes that change the scope of the claims, 3 examples of this can be found above, which include claims dated 2/28/05, 8/15/05, and 12/19/05.

14. The Applicant states that Emigh does not disclose or suggest a master system, which monitors the integrity of a security subsystem. The Examiner disagrees with the Applicant. The Examiner previously indicated in office action dated 10/17/05, that Emigh teaches a master system which monitors the integrity of a security subsystem, because Emigh teaches IBM which is the NSOC master system, will conduct testing of network devices for vulnerability (see pg. 1). The Applicant states that vulnerability is not the same as integrity. First, the Applicant has not provided in the disclosure a specific definition of the term integrity. Second, Emigh does teach

monitoring the integrity, because if a misuse is found the alarm will be sent to the master system(see pg. 1). Furthermore, the NSOC(i.e. master system) monitors, the network using the Netranger sensor(see pg. 1). Just for arguments sake, if the Examiner were to agree with the Applicant that "integrity relates to whether the device is in a state of being unimpaired". Emigh does teach the security subsystem(i.e. sensor) is in a state of being unimpaired, because an intrusion was detected(see pg. 1).

15. The Applicant states that Emigh does not disclose a security subsystem that monitors activities of devices on a network. The Examiner disagrees with the Applicant. Netranger(i.e. security subsystem) monitors devices on the network, because Netranger is located on places within the corporate network such as Internet and Intranet connections(see pg. 1). These connections more than one, according to Emigh, monitor traffic which is activities of these devices, these activities are intrusions/misuse, and if an intrusion is found an alarm is sent to the NSOC. Second, the Applicant is arguing certain type of attacks that may undetected. This point is moot. The claims stated, "detect attacks on the at least some devices". The claim does not distinguish between what type of attacks.

16. Further, the Examiner previously indicated objected to claims, objected because claims depend from rejected base claims. In order to advance prosecution of this Application, Applicant is urged to look closely at objected to claims 31, 36-37. If the Applicant were to incorporate the limitations of these claims into the independent claims, prosecution probably would be advanced. The Applicant is also urged to look at page 5 of specification, lines 15-25. These concepts are also illustrated in the dependent claims above, if re-written prosecution would probably be

advanced. The Examiner uses the word "probably", because if the changes were made, the application has to be reviewed before it is allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

January 11, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100